修 士 論 文 の 和 文 要 旨

大学院　電気通信学研究科　博士前期課程　情報通信学専攻		
氏　　名	根岸 大宙	学籍番号 0430032
論 文 題 目	多重線形解読法におけるメッセージ数と解読ビット数の評価	

要　旨

共通鍵暗号はブラウザやICカードに実装されており、実際に広く用いられている暗号技術のひとつである。共通鍵暗号は暗号の安全性に関する研究も多くおこなわれており、差分解読法や線形解読法などの強力な解読法が数多く提案されている。

本論文で取り上げる線形解読法は1993年に提案された共通鍵暗号に対する強力な解読法であり、世界で始めて米国標準暗号 DES を解読した解読法である。線形解読法は暗号化関数を線形関数で近似し、近似された線形関数と大量のメッセージ組を用いる事によって暗号化に用いた鍵を解読する解読法である。
また線形解読法を改良した多重線形解読法が2004年に提案された。多重線形解読法は複数の暗号化関数の近似式を複数用いて解析をおこなうことで、多くの情報を得ることや、解読に用いるメッセージ数を減らす事が出来る解読法である。

本論文では小規模な暗号を実装し、その暗号に線形解読法と多重線形解読法による解析をおこなうことによって、二つの解読法の比較をおこなう。しかし線形解読法と多重線形解読法は解読によって得られる情報量が異なるため、解読の成功確率だけで比較する事は妥当ではない。よって本論文では異なる情報量を求める事が出来る解読法の比較をおこなうため、解読済みのビット数を成功確率から求める方法について検討する。その上で実験結果から解析後の解読ビット数を評価することによって、線形解読法と多重線形解読法の比較をおこなう。